(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 49 440 A 1**

(51) Int. Cl.[7]:
G 06 F 11/30
G 05 B 15/02
G 05 B 19/048

(21) Aktenzeichen: 100 49 440.4
(22) Anmeldetag: 6. 10. 2000
(43) Offenlegungstag: 11. 4. 2002

(71) Anmelder:
DaimlerChrysler AG, 70567 Stuttgart, DE

(72) Erfinder:
Heinzler, Stefan, Dipl.-Ing.(FH), 88069 Tettnang, DE;
Rahm, Martin, Dipl.-Ing.(FH), 70563 Stuttgart, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	197 12 375 A1
US	54 08 643
WO	96 20 103 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zum Betrieb eines von einem Prozessor gesteuerten Systems

(57) Vorgeschlagen wird ein einfaches und kostengünstiges Verfahren zur Überwachung eines insbesondere sicherheitskritischen Systems.
Hierzu wird durch Verwendung mindestens einer Programmroutine des Prozessors mindestens ein Triggerwert berechnet, mittels dem eine Watchdog-Einheit rückgesetzt wird.
Verfahren zum Betrieb einer von einem Prozessor gesteuerten sicherheitskritischen Bedienfunktion eines Kraftfahrzeugs.

DE 100 49 440 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Betrieb eines von einem Prozessor gesteuerten Systems nach dem Oberbegriff des Patentanspruchs 1 wie es aus der DE 198 47 986 A1 bekannt ist.

[0002] Prozessorgesteuerte Systeme, bsp. durch Mikroprozessoren oder Mikrocontroller gesteuerte Systeme, werden insbesondere zur Realisierung bestimmter Anwendungen eingesetzt, wie bsp. zur Realisierung vorgegebener Funktionen oder Abläufe. Durch einen Fehler im System, bsp. durch eine Fehlfunktion im Prozessor oder einen Bitfehler in der Speichereinheit des Systems, kann ein Anwendungsfehler auftreten, bsp. ein falscher Ablauf oder eine nicht beabsichtigte Funktion realisiert und ausgeführt werden. Dieses Fehlverhalten ist unerwünscht und störend und muß insbesondere bei prozessorgesteuerten Systemen zur Realisierung sicherheitskritischer Anwendungen (bei Kraftfahrzeugen bsp. den Tempomat, den Airbag oder die Lenkwinkelerkennung betreffende Anwendungen) ausgeschlossen werden.

[0003] Um Fehlverhalten des Systems zu erkennen und/oder auszuschließen, insbesondere bei sicherheitskritischen Anwendungen, können dem System mehrere Prozessoren zugeordnet werden. Hierbei können die Prozessoren sich gegenseitig überwachen und das System außer Funktion setzen, wenn von einem Prozessor eine Fehlfunktion eines anderen Prozessors erkannt wird, insbesondere wenn jedem der Prozessoren nur ein Teil der Anwendung zugeordnet wird oder wenn neben einem "Hauptprozessor" ein "Hilfsprozessor" mit Überwachungsaufgaben vorgesehen wird. Nachteilig bei diesen Mehrprozessorsystemen sind einerseits die zusätzlichen Kosten und andererseits der erhöhte Aufwand für Hardware.

[0004] Beim Einprozessorsystem der gattungsbildenden DE 198 47 986 A1 sind zur Fehlerüberwachung zwei voneinander unabhängige dem Prozessor zugeordnete Watchdog-Einheiten vorgesehen, durch die beim Feststellen eines Fehlers das System in einen Fehlerreaktionszustand versetzt wird; aufgrund der beiden Watchdog-Einheiten fallen auch hier hohe Kosten und ein erhöhter Aufwand an Hardware an.

[0005] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Betrieb eines von einem Prozessor gesteuerten Systems gemäß dem Oberbegriff des Patentanspruchs 1 anzugeben, bei dem der korrekte Betrieb des Systems, insbesondere für sicherheitskritische Anwendungen, auf einfache und kostengünstige Weise überwacht werden kann.

[0006] Diese Aufgabe wird erfindungsgemäß durch das Merkmal im Kennzeichen des Patentanspruchs 1 gelöst.

[0007] Vorteilhafte Ausgestaltungen des Verfahrens sind Bestandteil der weiteren Patentansprüche.

[0008] Der Erfindung liegt die Erkenntnis zugrunde, daß in vielen prozessorgesteuerten Systemen (insbesondere zur Realisierung sicherheitskritischer Anwendungen wie in der DE 198 47 986 A1) eine als Watchdog oder Watchdog-Schaltung mit mindestens einem Watchdog ausgebildete Watchdog-Einheit vorgesehen ist, um undefinierte Zustände des Systems (bsp. Endlosschleifen in der Software aufgrund eines fehlerhaften Operationscodes) zu erkennen und durch ein Rücksetzen des Systems (einen Reset) zu beenden.

[0009] Erfindungsgemäß muß die Watchdog-Einheit zur Vermeidung eines Rücksetzens (Resets) des von einem Prozessor gesteuerten Systems während der Programmlaufzeit des Prozessors zur permanenten Überprüfung des Prozessors zyklisch mit mindestens einer von mindestens einem Triggerwert abhängigen Ausgangsgröße beaufschlagt werden. Der mindestens eine Triggerwert wird durch Verwendung mindestens einer Programmroutine des Prozessors berechnet, insbesondere nach Durchlaufen mindestens einer Programmroutine des Prozessors; insbesondere wird der Triggerwert von der zentralen Prozessoreinheit (CPU) berechnet, d. h. die Programmroutine wird in der zentralen Prozessoreinheit (CPU) durchlaufen. Als von den Triggerwerten abhängige Ausgangsgröße kann hierbei bsp. eine Pulsfolge und/oder ein bestimmtes Zeitfenster und/oder ein Funktionswert (eine Zeichenfolge) herangezogen werden, die zum Rücksetzen der Watchdog-Einheit vorgesehen werden; d. h. die Watchdog-Einheit vergleicht die im Prozessor (insbesondere in der CPU) generierten und bsp. in eine Pulsfolge und/oder ein Zeitfenster und/oder einen Funktionswert (Zeichenfolge) als Ausgangsgröße umgesetzten Triggerwerte mit einem intern gespeicherten Vergleichsmuster und wird bei einer Übereinstimmung von Ausgangsgrößen und Vergleichsmuster zurückgesetzt. Somit wird der mindestens eine Triggerwert für die Watchdog-Einheit und damit die (bsp. als Zeitfenster und/oder Funktionswert ausgebildete Ausgangsgröße) nicht bereits während der Codierung des Prozessors fest vorgegeben, sondern während des Betriebs des Prozessors ständig neu berechnet; da die mindestens eine Programmroutine des Prozessors zur Berechnung der Triggerwerte mit solchen Eingangsgrößen aufgerufen wird, daß die aus den Triggerwerten bestimmten Ausgangsgrößen bei korrekter Funktion des Prozessors dem Vergleichsmuster der Watchdog-Einheit entsprechen, werden beim Auftreten eines Fehlers im Prozessor die aus den Triggerwerten bestimmten Ausgangsgrößen nicht dem in der Watchdog-Einheit gespeicherten Vergleichsmuster entsprechen; hierdurch wird die Watchdog-Einheit fehlerhaft angesteuert (insbesondere nicht zurückgesetzt) und erzwingt hierdurch einen Reset des Systems.

[0010] Als Programmroutine zur Berechnung der Triggerwerte kann eine Testfunktion verwendet werden, die zumindest einen Teil der Operationen aus dem Befehlssatz der zentralen Prozessoreinheit (CPU) ausführt, bsp. typische CPU-Operationen wie Additionen, Schiebeoperationen oder Bitmanipulationen; vorzugsweise werden hierzu alle Operationen aus dem Befehlssatz der zentralen Prozessoreinheit (CPU) ausgeführt. Insbesondere bei prozessorgesteuerten Systemen zur Realisierung sicherheitskritischer Anwendungen wird als Programmroutine zur Generierung der Triggerwerte mindestens eine sicherheitskritische Programmroutine ganz oder zumindest teilweise durchlaufen, so daß auf diese Weise eine permanente Überwachung kritischer Anwendungen (Funktionen oder Abläufe) stattfindet.

[0011] Die Watchdog-Einheit als eigenständige Funktionseinheit des prozessorgesteuerten Systems kann hierbei entweder im Prozessor angeordnet sein (mit den Funktionseinheiten des Prozessors im Prozessor integriert werden) – in diesem Falle können die Funktionseinheiten des Prozessors (bsp. kann neben dem Watchdog und der zentralen Prozessoreinheit noch eine Recheneinheit und eine Speichereinheit vorgesehen werden) über die Leitungen eines internen Bussystems verknüpft werden, wobei insbesondere auch die Verbindung zwischen der zentralen Prozessoreinheit und der Watchdog-Einheit über das Bussystem erfolgen kann – oder aber außerhalb des Prozessors angeordnet sein, d. h. neben dem Prozessor eine weitere Komponente des Systems bilden – in diesem Falle kann die Verbindung zwischen der zentralen Prozessoreinheit und der Watchdog-Einheit über eine externe Datenleitung erfolgen.

[0012] Vorteilhafterweise kann mit dem vorgestellten Verfahren ein (insbesondere sicherheitskritisches) System und die korrekte Ausführung der Systemfunktion ohne das Erfordernis zusätzlicher Hardware und damit auf einfache und kostengünstige Weise überwacht werden.

[0013] Im Zusammenhang mit der Zeichnung soll das Verfahren weiter erläutert werden. Hierbei zeigt die Figur ein Ausführungsbeispiel der Komponenten eines als Mikrocontroller ausgebildeten Prozessors zur Steuerung sicherheitskritischer Bedienfunktionen bei einem Kraftfahrzeug.

[0014] Der Mikrocontroller **1** als Einprozessorsystem ist bsp. zum Einlesen von Steuerdaten und damit zur Steuerung eines als Tempomat eines Kraftfahrzeugs ausgebildeten Systems vorgesehen. Der Mikrocontroller **1** weist gemäß der **Fig.** 1 als Funktionseinheiten bsp. eine Zentrale Prozessoreinheit **3** (CPU), eine Speichereinheit **4** und eine Recheneinheit **6** auf; die Funktionseinheiten des Mikrocontrollers **1** sind über die Busleitungen **7** des Bussystems **2** zum Austausch von Datensignalen und Steuersignalen intern miteinander verknüpft.

[0015] Weiterhin ist im Mikrocontroller **1** ein Watchdog **5** vorgesehen, der ebenfalls an die Busleitungen **7** des Bussystems **2** angeschlossen ist; dieser Watchdog **5** muß zyklisch getriggert werden, um einen Reset des Systems zu verhindern. Hierzu muß der Watchdog **5** bsp. zyklisch alle 20 ms innerhalb eines vorgegebenen Zeitraums (innerhalb eines bestimmten Zeitfensters) von bsp. 2 ms mit einer vorgegebenen Zeichenfolge von bsp. 55_H, AA_H beaufschlagt werden. Zur Realisierung der Triggerung des Watchdogs **5** werden während der Programmlaufzeit des Mikrocontrollers **1** Triggerwerte TW permanent neu berechnet, indem von der CPU **3** des Mikrocontrollers **1** eine in der Speichereinheit **4** des Mikrocontrollers **1** abgelegte Funktion F aufgerufen wird (Schritt (a)) und mittels dieser Funktion F von der CPU **3** unter Verwendung eines bestimmten Startwerts durch Heranziehen aller arithmetischen Befehle aus dem Befehlssatz der CPU **3** aus den berechneten Triggerwerten TW als Ausgangsgrößen AG ein Zeitintervall und eine Zeichenfolge abgeleitet werden. Diese Ausgangsgrößen AG werden an den Watchdog **5** gesandt (Schritt (b)) und von diesem mit dem im Watchdog **5** gespeicherten Vergleichsmuster verglichen: entsprechen die Ausgangsgrößen AG dem Vergleichsmuster, d. h. wird der Watchdog **5** nach 20 ms (im Zeitfenster zwischen 19 ms und 21 ms) mit der Zeichenfolge 55_H, AA_H beaufschlagt, wird der Watchdog **5** neu getriggert (zurückgesetzt); entsprechen die Ausgangsgrößen AG nicht dem Vergleichsmuster (bsp. aufgrund eines Fehlers im Mikrocontroller **1**), d. h. wird der Watchdog **5** entweder nicht nach 20 ms (nicht im Zeitfenster zwischen 19 ms und 21 ms) oder nicht mit der Zeichenfolge 55_H, AA_H beaufschlagt, wird der Watchdog **5** nicht neu getriggert, d. h. er wird nicht zurückgesetzt und führt daher einen Reset des Systems durch.

Patentansprüche

1. Verfahren zum Betrieb eines von einem Prozessor (**1**) gesteuerten Systems, bei dem eine Watchdog-Einheit (**5**) zur Verhinderung eines Rücksetzens des Systems vom Prozessor (**1**) zyklisch zurückgesetzt werden muß, **dadurch gekennzeichnet**, daß durch Verwendung mindestens einer Programmroutine des Prozessors (**1**) mindestens ein Triggerwert (TW) berechnet wird, und daß das Rücksetzen der Watchdog-Einheit (**5**) in Abhängigkeit des mindestens einen berechneten Triggerwerts (TW) erfolgt.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der mindestens eine Triggerwert (TW) von der zentralen Recheneinheit (**3**) des Prozessors (**1**) berechnet wird.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß zur Berechnung des mindestens einen Triggerwerts (TW) der gesamte Befehlssatz der zentralen Recheneinheit (**3**) des Prozessors (**1**) verwendet wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß zur Berechnung des mindestens einen Triggerwerts (TW) mindestens eine sicherheitskritische Programmroutine des Prozessors (**1**) verwendet wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß in Abhängigkeit des Triggerwerts (TW) ein Zeitfenster als Ausgangsgröße (AG) bestimmt wird, innerhalb dessen die Watchdog-Einheit (**5**) zurückgesetzt werden muß.
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß in Abhängigkeit des Triggerwerts (TW) eine Zeichenfolge als Ausgangsgröße (AG) bestimmt wird, mit der die Watchdog-Einheit (**5**) beaufschlagt werden muß.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Watchdog-Einheit (**5**) im Prozessor (**1**) integriert wird.
8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die Watchdog-Einheit (**5**) mit den Funktionseinheiten (**3**, **4**, **6**) des Prozessors (**1**) über ein Bussystem (**2**) verbunden wird.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 100 49 440 A1
Int. Cl.: G 06 F 11/30
Offenlegungstag: 11. April 2002

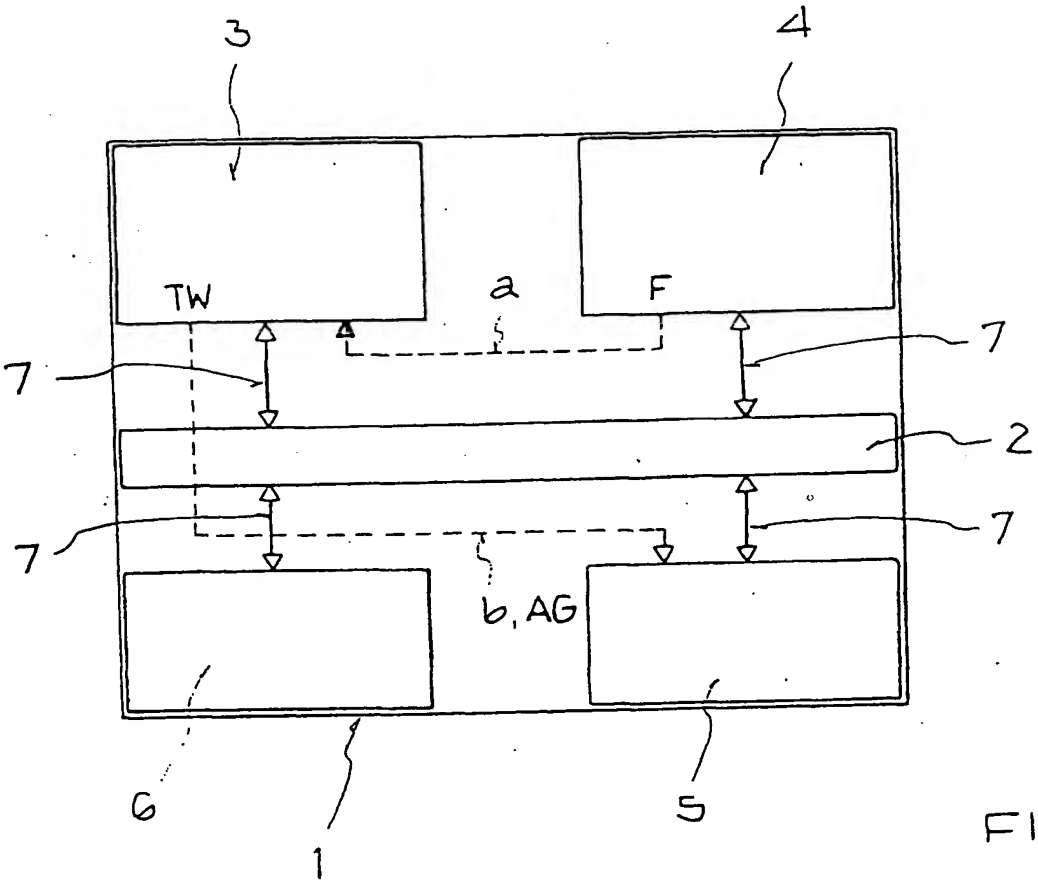


FIG.

1.

AN: PAT 2002-406538

TI: Watchdog unit resetting method for e.g. vehicle applications, involves calculating trigger value which is used for resetting unit

PN: **DE10049440**-A1

PD: 11.04.2002

AB: NOVELTY - The method involves calculating a trigger value (TW) by using preferably, the CPU (3) of the processor (1). The watchdog unit (5), which prevents resetting the system by the processor is reset dependent on the calculated trigger value. Preferably, the watchdog unit is integrated in the processor and connected to the CPU, storage unit (4) and calculation unit (6) of the processor via a bus system (2).; USE - For processor controlled systems especially for security critical application, such as automatic speed control, airbag or steering angle detection. ADVANTAGE - Allows monitoring of systems in simple and cost-effective manner. DESCRIPTION OF DRAWING(S) - The drawing shows the components of a processor for controlling security critical functions of a vehicle. Processor 1 Bus system 2 CPU 3 Storage unit 4 Watchdog unit 5 Calculation unit 6

PA: (DAIM) DAIMLERCHRYSLER AG;

IN: HEINZLER S; RAHM M;

FA: **DE10049440**-A1 11.04.2002;

CO: DE;

IC: G05B-015/02; G05B-019/048; G06F-011/30;

MC: T01-J07D1; X22-J07; X22-X06H;

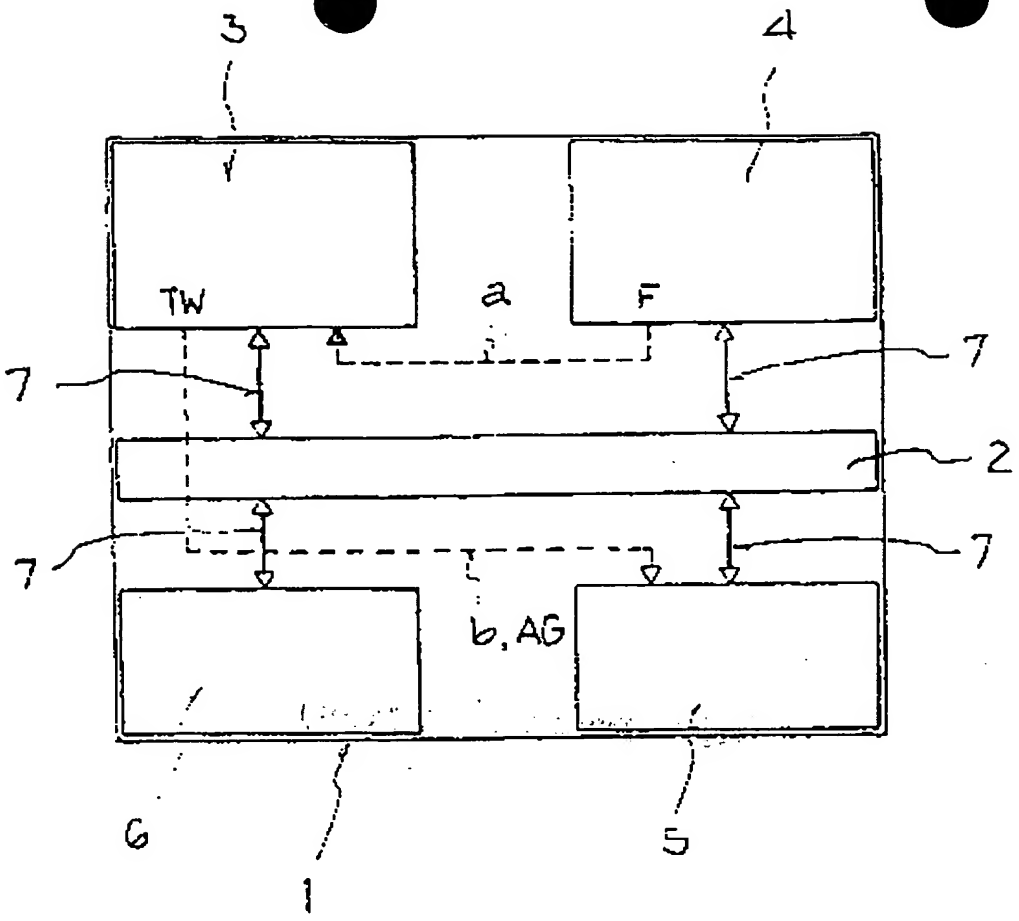
DC: T01; X22;

FN: 2002406538.gif

PR: DE1049440 06.10.2000;

FP: 11.04.2002

UP: 11.07.2002



THIS PAGE BLANK (USPTO)

DOCKET NO: 53-02P14830
SERIAL NO: 10/535,126
APPLICANT: Graßhoff et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100